Strategien zur Behandlung aktueller Entwicklungen im Bereich Viren- und SPAM-Erkennung

Benutzung des Dienstes e-Mail unter verschärften Bedingungen

Joachim Ritschel

Workshop 11.5.2005 TU Ilmenau

SMTP history

- Das Protokoll zum Transport von Email im Internet ist das SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) – Protokoll.
- Kommunikation MTA zu MTA oder Mailklient zu MTA
- Dieses Protokoll wurde im Jahre 1982 eingeführt und ist damals im RFC 821 (http://www.ietf.org/rfc/rfc0821.txt?number=821) beschrieben worden .
- Im Jahre 2001 wurde das Protokoll dann aktualisiert; seitdem gehört auch der RFC 2821 (http://www.ietf.org/rfc/rfc2821.txt) zum Standard

SMTP history

- Wesentliche Funktionserweiterung durch
  E-Mails mit Attachment

- MIME (**M**ultipurpose **I**nernet **M**ail **E**xtention)
  http://www.iana.org/assignments/media-types/

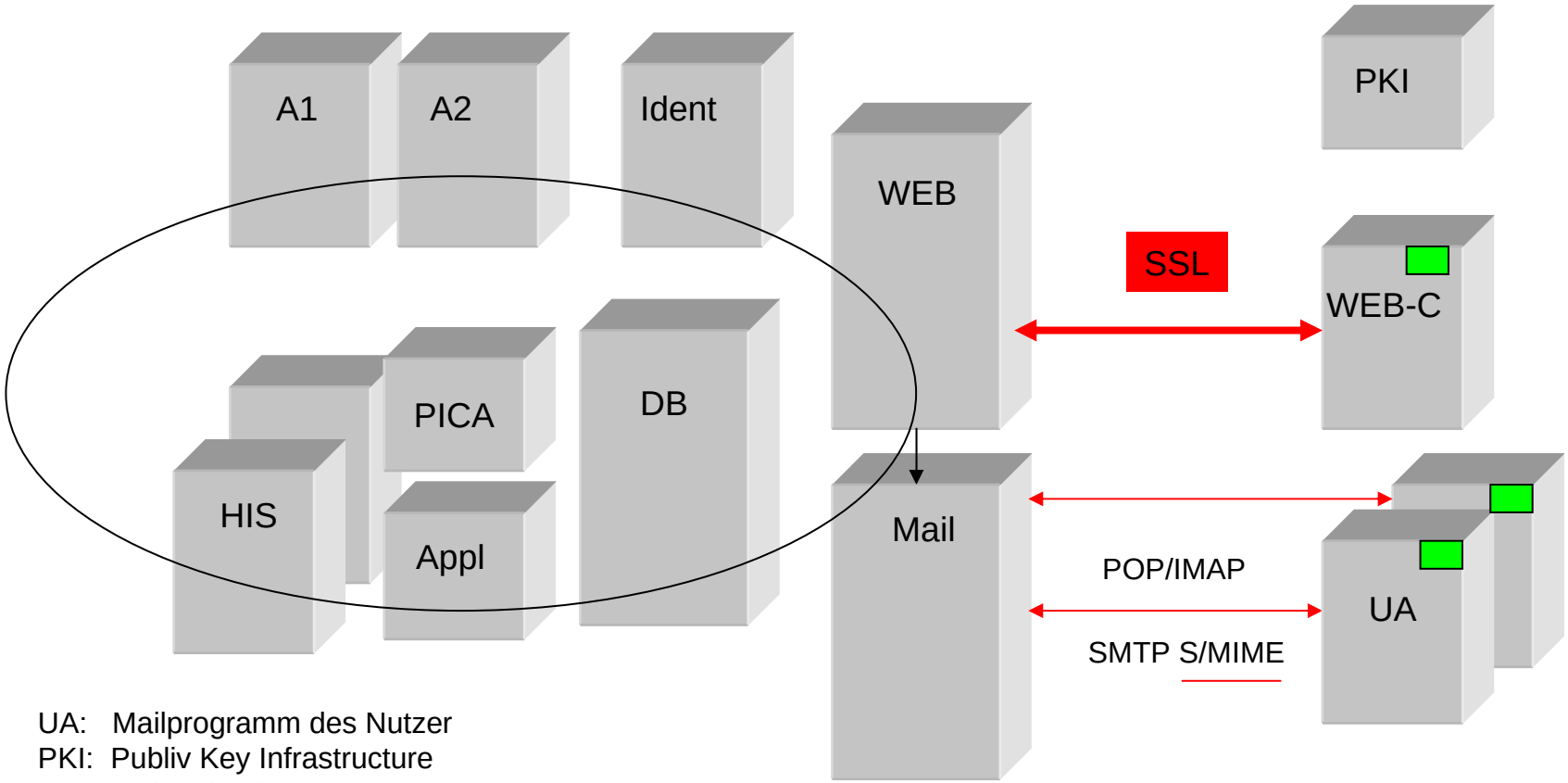
- Beim Empfang ist eine einfache Anzeige/Wiedergabe des
  Anhangs möglich

Die SMTP Erfolgsgeschichte

- Textbasiert
- Einfach zu implementieren
- Texte oder beliebige Anhänge lassen sich ohne spezielle Rechte austauschen
- Kostenlose Produkte für Server (MTA) und Mailprogramme (UA)
- Weltweite Verbreitung – sehr große Community
- Implementierung von UA auf modernen mobilen Geräten (PDA/Handy)
- Implementierung in zahlreichen Softwareprodukten
- Die Kommunikation per E-Mail wurde in Workflows integriert

- ***Fazit: Ein Ausfall des Dienstes hat Folgen !***

SMTP im Kontext typischer IT-Umgebungen von Hochschulen



UA: Mailprogramm des Nutzer
PKI: Publiv Key Infrastructure
A1: Authentication Server
A2: Authorization Server
Ident:Verzeichnis der Identitäten (Personen)
Appl: Application Server

Schwächen

Brief	E-Mail
Absender ist auf dem Briefumschlag	Absenderadresse (SMTP) ist nur dem Postmaster bekannt (Logfiles) Absender Nicht im From: Feld
Empfänger ist auf dem Briefumschlag	Empfängeradresse (SMTP) ist im Envelope enthalten Nicht im To:-Feld !!!
Stempel für Zeit und Ort: Poststempel	Envelope Kann leicht gefälscht werden !!
Briefbogen mit Kopf und Inhalt Unterschrift	From:-Feld, To:-Feld, Subject, Text, Anhänge, Unterschrift nicht möglich !!

Tabelle1: E-Mail und die Analogie zur gelben Post

Schwächen

- telnet mail.tu-ilmenau.de 25
- HELO mail.tu-ilmenau.de
- MAIL FROM: 134578964@gmx.de
- RCPT TO: paul.mustermann@tu-ilmenau.de
- DATA
- FROM: Hostmaster@tu-ilmenau.de
- TO: fg-leiter-tu-ilmenau@tu-ilmenau.de
- Subject: Wartungstermin am 1.5.2005
- <Leerzeile>
- Das Netzwerk der TU Ilmenau steht am 1.5.2005 wegen dringender Arbeiten am Netzwerk nicht zur Verfügung. Bitte planen Sie evtl. Ihre Lehrveranstaltungen ……
- .
- QUIT

Beispiel für das Fälschen von Empfänger und/oder Senderadresse einer E-Mail

Schwächen

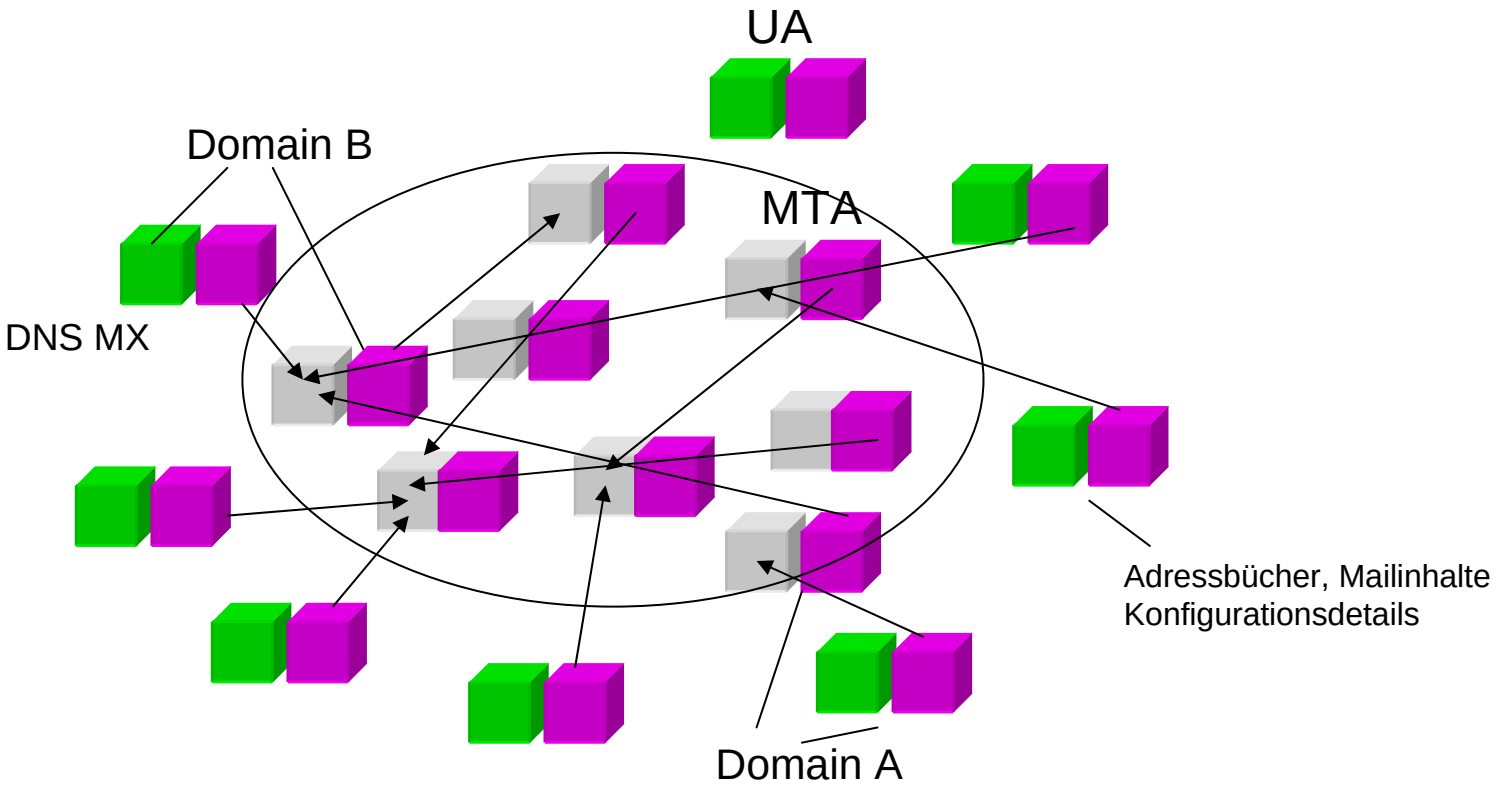
- Die Authentizität von Absender und Inhalt ist nicht nachprüfbar

Unerwünschte Massenmails, virenbehaftete Mails

- **Ziel:**
  - Konsumverhalten ausspionieren (Spyware 70 %)
  - Informationen verbreiten
  - Fremde Ressourcen benutzen
  - Kommunikationswege verschleiern

- **Motivation:**
  - kommerziell
  - politisch
  - religiös
  - ……
  - selten: sozial

Die Sicht der SPAMMER



MTA SMTP-Server und SMTP-Klient)

UA IMAP-, POP-, SMTP-Klient)

Verändertes Benutzungsprofil

- Hohe Verfügbarkeit
- Datensicherung
- Höhere Quota am Mailboxserver
- Benutzung mit UA‘s an mehreren evtl. mobilen Geräten mit begrenzten lokalen Ressourcen und Anschlussbandbreiten
- Postfächer und serverbasierter Filterung (Sieve)
- Abwesenheitsmail, Mailweiterleitung (Sieve)
- Vorkonfiguration der SPAM Behandlung (Sieve)
- Teilautomatisierte Wartungsaufgaben

Verteidigung

- **Benutzer:**
  - Schulung
- **Arbeitsplatzrechner:**
  - Virenscanner mit aktuellen Pattern
  - Systemschwachstellen schließen
  - Softwarefirewall ???
  - Alternativen zum UA MSOutlook ? (Entschuldigung!)
- **Mailserver:**
  - RBL+
  - Greylisting
  - Authentication und Relayrecht (SMTP Auth, SmartCard)
  - Virenscanner für SMTP (90%)
  - SPAM Erkennung und Kennzeichnung
  - Automatische Auswertung der SPAM-Kennzeichnung am Server
  - Keine unmoderierten Mailverteiler
  - Restriktives Provisioning
- **Netzwerk:**
  - MX und zentraler Filter am Netzwerkzugang zum Internet

Verteidigung

- Am Mailserver:
  - MAPS RBL+ (Realtime Blackhole List Plus)
    - Informationen www.mailabuse.org
    - Einsatz an den Thüringer Hochschulen
    - Kostenpflichtige Datenbank
    - Verteilung per DNS
    - MAPS RBL (Realtime Blackhole List)
    - MAPS DUL (Dynamic User List)
    - MAPS RSS (Realy SPAM Stopper)
    - MAPS NML (Non confirmed Mailinglists)

Verteidigung

- Am Mailserver:
  - Greylisting:

    Mails von anderen MTA‘s werden erst nach einer Sendewiederholung abgenommen. Bekannte Systeme werden sofort bedient. !?

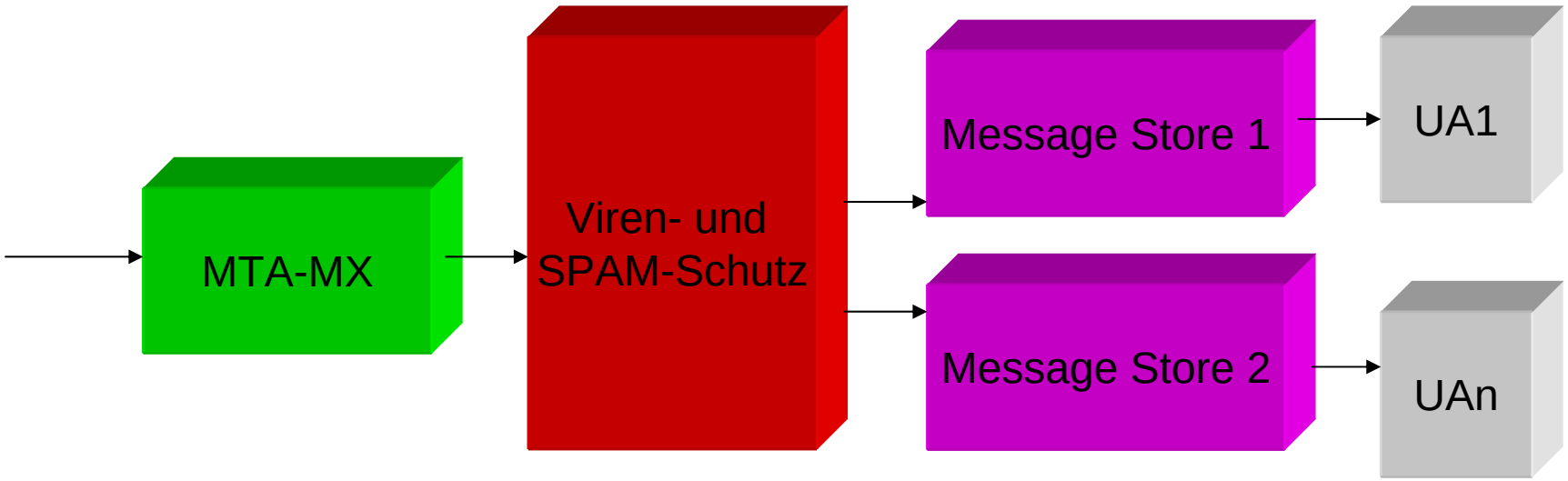
    - Problem:

      Belastung der Queueingressourcen

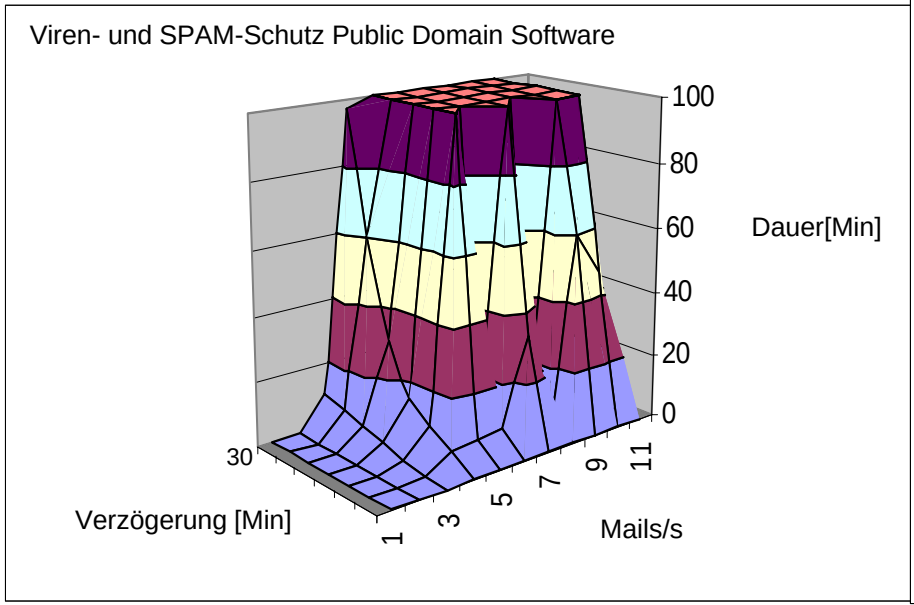
      sicherlich keine nachhaltig wirkende Strategie

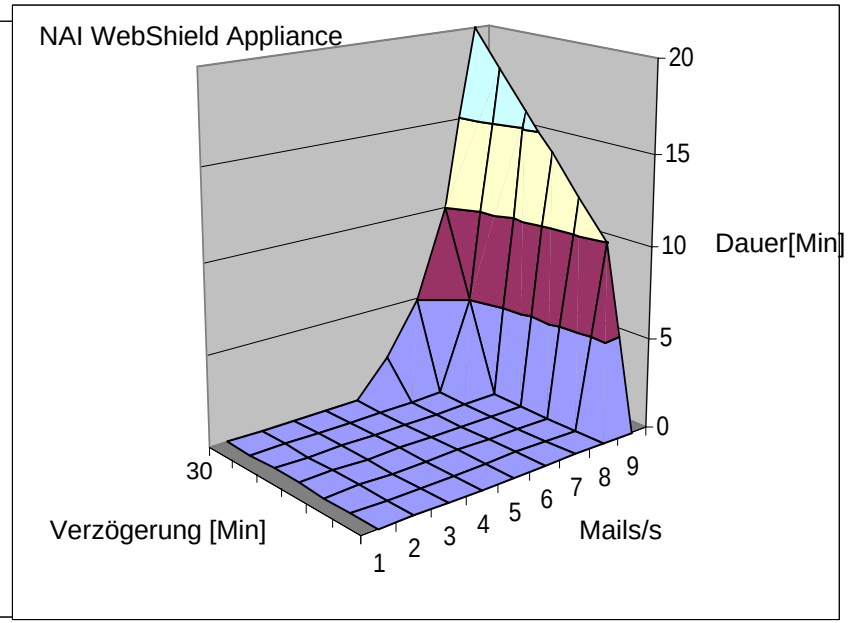
Verteidigung

- Am Mailserver:
  - Viren- und SPAM-Erkennung



Lastverhalten der Viren- und SPAM-Erkennung





NAI WebShield Appliance

- Hardware-/Softwarelösung
- Im Transparentmodus ist der Schutz auf Netzwerkebene möglich
- Einsatz an den Thüringer Hochschulen
- Erweiterter Einsatz für HTTP und FTP ist möglich
- Gute Skalierung beim Eintreffen von Massenmails
- OS und Patternfiles werden vom Hersteller bereitgestellt
- Der Betrieb ist weitestgehend automatisiert
- Grafische Reports
- Sehr flexible Gestaltung der Policies:
  - Vererbungsmechanismus
  - Nutzergruppen
  - Speziele Behandlung von:
    - Eingehende oder ausgehende Mails
    - Ungültig signierten Mails
    - Verschluesselten oder anders geschützten Inhalten
    - Defekten Anhängen
  - Benachrichtgungsvarianten/flexible Gestaltung der Benachrichtigungstexte
  - Quarantäne/Entfernen von Anhängen/Entfernen von schädlichen Teilmengen eines Anhanges
- Es gibt eine GUI für administrative Zwecke

Die Befriedigung der veränderten Benutzungsprofile

- Hohe Verfügbarkeit:
  Redundanzen bei Netzteilen und HD
  RAID1 RAID5
- Datensicherung: täglich zentrales Backup
- Quota 400MByte für Mitarbeiter/100MByte für Studenten
- Neben POP wird auch IMAP (TLS optional) geboten
- Webmail mit GUI für Abwesenheitsmails, Weiterleitungen, Mailfilter am Server (Sieve - nur für Mitarbeiter)
- Teilautomatisierte Wartungsaufgaben per Webmail
- Relayrecht für Universitätsangehörige per SMTP AUTH oder TLS Klient (SmartCard)
- Vorkonfiguration SPAM Behandlung:
  X-NAI-SPAM-LEVEL: **** → INBOX.SPAM